

On some power sum problems of Montgomery and Turán

Johan Andersson*

February 5, 2008

Abstract

We use an estimate for character sums over finite fields of Katz to solve open problems of Montgomery and Turán. Let $h \geq 2$ be an integer. We prove that $\inf_{|z_k|=1} \max_{\nu=1, \dots, n^h} |\sum_{k=1}^n z_k^\nu| \leq (h-1+o(1))\sqrt{n}$. This gives the right order of magnitude for the quantity and improves on a bound of Erdős-Rényi by a factor of the order $\sqrt{\log n}$.

1 Introduction

One of the simplest and most striking problems in the Turán power sum theory is to determine the quantity

$$(\star) = \inf_{|z_k|=1} \max_{\nu=1, \dots, m} \left| \sum_{k=1}^n z_k^\nu \right|$$

for various choices of integers n, m . The purpose of this paper is to find the correct order of magnitude for this quantity when $m \sim n^B$. For any fixed $B > 1$ and $m = \lfloor n^B \rfloor$ we prove that $(\star) \asymp \sqrt{n}$. This solves open problems of Hugh Montgomery and Paul Turán.

We first present some well known results about (\star) . By letting

$$z_k = e\left(\frac{k}{n}\right), \quad (e(x) = e^{2\pi i x})$$

we see that $(\star) = 0$ if $1 \leq m \leq n-1$. Turán [13] proved that $(\star) = 1$ if $m = n$. In general it is difficult to determine the quantity (\star) exactly but in [2] we proved that $(\star) = \sqrt{n-1}$ if $m = n^2 - n$ and $n-1$ is a prime power, and if $m = n^2 - j$ for $2 \leq j \leq n-1$ and n is a prime power then $(\star) = \sqrt{n}$.

*Email:johana@math.su.se

When exact values can not be determined we are interested in obtaining asymptotic estimates for (\star) when $n, m \rightarrow \infty$. In the special case $n^{1+\delta} < m \leq n^2$ we have proved in [3] that $(\star) \sim \sqrt{n}$.

Finding asymptotic estimates can be quite difficult as well and the next question is to ask for choices of m, n where we can find the order of magnitude for (\star) . Montgomery proved ([12], page 100, Theorem 10) that

$$\sqrt{nB} \ll \max_{\nu=1, \dots, n^B} \left| \sum_{k=1}^n z_k^\nu \right| \quad (1)$$

uniformly for $1 + \delta \leq B \leq n$ when $|z_k| = 1$. Erdős-Renyi [9] have used probabilistic reasoning to show that there exists an n -tuple (z_1, \dots, z_n) of unimodular complex numbers such that

$$\left| \sum_{k=1}^n z_k^\nu \right| \leq \sqrt{6n \log(m+1)} \quad (\nu = 1, \dots, m) \quad (2)$$

thus giving a general upper bound for (\star) . Let us now consider the case $m = \lfloor n^B \rfloor$ for a fixed constant $B > 1$. Leenman-Tijdeman [11] have given an explicit construction which yields the same order of magnitude as Eq. (2). Unfortunately these upper estimates differ by a essentially a $\sqrt{\log n}$ factor from the lower bound Eq. (1). This inspired Hugh Montgomery to state the following problem

Problem 1. (Montgomery, [12], page 197, Problem 13) Show that for any positive B there exist complex numbers z_1, \dots, z_n such that $|z_k| = 1$ for all k and

$$\left| \sum_{k=1}^n z_k^\nu \right| \ll_B \sqrt{n}. \quad (\nu = 1, \dots, \lfloor n^B \rfloor)$$

In contrast Turán had previously stated the following problem.

Problem 2. (Turán, [14] page 197, Problem 54) Does there exist an $w(x) \nearrow \infty$ such that

$$b_j > 0, \quad |z_j| = 1, \quad j = 1, \dots, n$$

implies for $g(\nu) = \sum_{j=1}^n b_j z_j^\nu$ the inequality

$$\max_{1 \leq \nu \leq n^{100}} |g(\nu)| > \frac{w(n)}{\sqrt{n}} |g(0)|?$$

If we can solve Montgomery's problem for $B = 100$ it is clear that there does not exist such a function $w(x)$ in Turán's problem. These conflicting guesses and a general lack of understanding of the situation has meant that until very recently it has not been clear to us what the correct order of magnitude in the problem should be. See the discussion in arXiv version 2 of [3].

2 Main results

The purpose of this paper is to solve Montgomery's problem and give the right order of magnitude for (\star) if $m = \lfloor n^B \rfloor$. We will use an estimate of character sums over finite fields of Katz. Before we state our theorems we state the following Lemma which we will prove in Section 3.

Lemma 1. *Let $h \geq 2$ be an integer and let q be a prime power. Then there exists unimodular complex numbers z_1, \dots, z_q such that*

$$\max_{\nu=1, \dots, q^h-2} \left| \sum_{k=1}^q z_k^\nu \right| \leq (h-1)\sqrt{q}.$$

We first state a non explicit version of our result which has a somewhat easier proof than our sharpest version.

Theorem 1. *Let $\delta > 0$. Then we have uniformly for $1 + \delta \leq B \leq n$ the following estimate*

$$\sqrt{Bn} \ll \inf_{|z_k|=1} \max_{\nu=1, \dots, \lfloor n^B \rfloor} \left| \sum_{k=1}^n z_k^\nu \right| \ll B\sqrt{n}.$$

If $|z_k| = 1$ is replaced by $|z_k| \geq 1$ then the result still holds for $2 \leq B \leq n$.

This Theorem gives a direct solution to Problem 1 of Montgomery and improves on Erdős-Renyi's result Eq. (2) for $2 < B \ll \log n$ by removing a factor $\sqrt{(\log n)/B}$.

Proof. The lower bound is Eq. (1). For the upper bound it is sufficient to consider $B = h$ for integers $h \geq 2$. Since 2^m is a prime power we can choose $\{z_{k,m}\}_{k=1}^{2^m}$ in Lemma 1 such that

$$\left| \sum_{k=1}^{2^m} z_{k,m}^\nu \right| \leq \left(\left\lceil \frac{N}{m} \right\rceil - 1 \right) 2^{m/2}. \quad (\nu = 1, \dots, 2^N - 2)$$

If $a_m = 0, 1$ are the digits in the binary expansion of n , i.e. $n = \sum_{m=0}^M a_m 2^m$, then the sum $\sum_{m=0}^M a_m \sum_{k=1}^{2^m} z_{k,m}^\nu$ is a power sum of n elements and can be written as $\sum_{k=1}^n z_k^\nu$. By the triangle inequality it is clear that

$$\left| \sum_{k=1}^n z_k^\nu \right| \leq \sum_{m=0}^M a_m \left(\left\lceil \frac{N}{m} \right\rceil - 1 \right) 2^{m/2} \ll \frac{N}{M} 2^{M/2}$$

for $\nu = 1, \dots, 2^N - 2$. By the binary expansion of n we have that $n \leq 2^{M+1} - 1$ and we see that $n^h \leq 2^N - 2$ when $n, h \geq 2$ and $N = h(M+1)$. We obtain the following estimate.

$$\left| \sum_{k=1}^n z_k^\nu \right| \ll h\sqrt{n}. \quad (\nu = 1, \dots, n^h)$$

□

Theorem 1 implies the following Corollary.

Corollary 1. *It is not possible to find a function $w(x)$ in Turán's problem, Problem 2.*

Proof. Choose $B = 100$ in Theorem 1 and $b_1 = \dots = b_n = 1$ in Turán's problem. □

We will now state a somewhat sharper version of Theorem 1, which we will choose to state for $|z_k| \geq 1$ instead of $|z_k| = 1$.

Theorem 2. *Let $h \geq 2$ be an integer and $\epsilon > 0$. One then has that*

$$C_h \sqrt{n} - O(n^{-1/2}) \leq \inf_{|z_k| \geq 1} \max_{\nu=1, \dots, n^h} \left| \sum_{k=1}^n z_k^\nu \right| \leq (h-1)\sqrt{n} + O(n^{0.2625+\epsilon}).$$

where $C_{2m} = (m!)^{1/2m}$ and $C_{2m+1} = C_{2m}$.

We will prove this Theorem in Section 4.

Remark 1. Theorem 2 still holds if $|z_k| \geq 1$ is replaced by $|z_k| = 1$ since the construction that yields the upper bound uses unimodular complex numbers. In this case the lower bound in Theorem 2 can be improved slightly by using the method from [4], e.g. for $h = 3$ we get the lower bound $\sqrt{2n}$ instead of \sqrt{n} . At present there is however no $h > 2$ where we can attain asymptotic estimates in the problem.

By choosing $h = 3$ in Theorem 2 (with $|z_k| = 1$) we get the following Corollary.

Corollary 2. *Let $\alpha > 1$ be a real number. One then has that*

$$\inf_{|z_k|=1} \max_{\nu=1, \dots, \lfloor \alpha n^2 \rfloor} \left| \sum_{k=1}^n z_k^\nu \right| \leq 2\sqrt{n} + O(n^{0.2625+\epsilon}). \quad (\epsilon > 0)$$

This improves on Theorems 6 and 7 from version 2 on arXiv of [3] for $\alpha > 4$.

Remark 2. In the proof of Theorem 2 we use the methods of [3], Section 6. The simpler methods of [3], Subsection 4.1 can be used to prove a weaker form of Theorem 2 that still implies the Corollary.

We will here suggest the following open problems (Compare with [3], Problem 3).

Problem 3. Find an increasing function $\Lambda(x)$ such that for each $B > 1$ one has that

$$\inf_{|z_k|=1} \max_{\nu=1, \dots, \lfloor n^B \rfloor} \left| \sum_{k=1}^n z_k^\nu \right| \sim \Lambda(B) \sqrt{n}.$$

Question 1. Is the upper bound in Theorem 2 sharp? Can we choose $\Lambda(h) = h - 1$ in Problem 3 when $h \geq 2$ is an integer?

Also the positive solution to Montgomery's problem suggests that the following problem might be possible to solve.

Problem 4. Let $h \geq 2$ be an integer. Find an increasing function $\Lambda_h(\alpha)$ such that for each $\alpha > 0$

$$\inf_{|z_k|=1} \max_{\nu=1, \dots, \lfloor \alpha n^h \rfloor} \left| \sum_{k=1}^n z_k^\nu \right| \sim \Lambda_h(\alpha) \sqrt{n}.$$

For $h = 2$ this is given as Conjecture 4 in [3].

Question 2. Assume that we can solve Problem 4. Is it true that $\lim_{\alpha \rightarrow \infty} \Lambda_h(\alpha) = \lim_{\alpha \rightarrow 0^+} \Lambda_{h+1}(\alpha)$?

If Question 2 is true and Problem 3 solvable then we have that the function $\Lambda(x)$ in Problem 3 is piece wise constant for $n < x < n + 1$.

3 Proof of Lemma 1

Proof. Let F be a finite field of order q and let E be an extension field of F of order q^h . Let x_1, \dots, x_q denote the elements of F . Let ω be an element that generates the multiplicative group E^* , and let χ be a multiplicative character on E of order $q^h - 1$. Choose

$$z_k = \chi(\omega + x_k). \quad (k = 1, \dots, q)$$

Then

$$\sum_{k=1}^q z_k^\nu = \sum_{x \in F} \chi_\nu(\omega + x), \quad (3)$$

where $\chi_\nu = \chi^\nu$ is a non trivial character on E unless $(q^h - 1) | \nu$. By Theorem 1 of Katz [10] its absolute value can be estimated from above by $(h - 1)\sqrt{n}$ for $\nu = 1, \dots, q^h - 2$. \square

Remark 3. The character sum Eq. (3) first occurred as eigenvalues of adjacency matrices of graphs in Chung [8]. Katz proof uses Weil's estimates [15], although he prefers to use the language of Deligne.

Remark 4. For $h = 2$ the construction in Lemma 1 coincides with our construction in Eq. (7) of [2], where we used a result of Bose [6] on B_2 sequences $(\text{mod } q^2 - 1)$. Bose's result has been generalized to B_h Sidon sequences $(\text{mod } q^h - 1)$ in Bose-Chowla [7], and this was how we originally arrived at the construction in Lemma 1. We will therefore describe the construction of Bose-Chowla. Let F and E be finite fields and ω an element in E which is a multiplicative generator for E^* as in the proof of Lemma 1. Choose the discrete logarithm so that $\log \omega = 1$. Let

$$a_k = \log(\omega + x_k). \quad (k = 1, \dots, q) \quad (4)$$

Then $\{a_k\}$ is a Sidon set of order h , or B_h set $(\text{mod } q^h - 1)$, or in other words the equation $a_{j_1} + \dots + a_{j_h} \equiv a_{i_1} + \dots + a_{i_h} \pmod{q^h - 1}$ has no non-trivial solution. Since the case $h = 2$ had been successfully used in the problem it was natural to expect that this construction could give good estimates for a general $h \geq 3$ and $\nu = 1, \dots, p^h - 2$. Indeed, numerical investigation (with $h = 3, 4$ and small primes) suggested to us that if

$$z_k = e\left(\frac{a_k}{q^h - 1}\right), \quad (k = 1, \dots, q)$$

then we should have

$$\left| \sum_{k=1}^q z_k^\nu \right| \leq (h-1)\sqrt{n}. \quad (\nu = 1, \dots, q^h - 2)$$

This can be explained as follows: We can define the character χ by

$$\chi(\omega^n) = e\left(\frac{n}{q^h - 1}\right), \quad \chi(0) = 0.$$

Then

$$z_k = \chi(\omega + x_k),$$

where χ is a character of order $q^h - 1$ on E^* as in the proof of Lemma 1.

4 Proof of Theorem 2

The lower estimate follows from Theorem 2 in our paper [1]

$$\left(\frac{n!m!}{(n-m)!}\right)^{1/(2m)} \leq \max_{\nu=1, \dots, n^{2m}} \left| \sum_{k=1}^n z_k^\nu \right|. \quad (|z_k| \geq 1)$$

Hence we will concentrate in proving the upper bound. We will use the method from [3]. We have the following Lemma:

Lemma 2. *Let $\epsilon > 0$, $0 < \theta < 1$, $C \geq 1$ and let $h \geq 2$ be an integer. Suppose that (z_1, \dots, z_n) is an n -tuple of unimodular complex numbers,*

$$m \sim n^\theta, \quad (5)$$

and

$$\left| \sum_{k=1}^n z_k^\nu \right| \leq C\sqrt{n}. \quad (\nu = 1, \dots, n^h)$$

Let $\mathcal{N} = \{1, \dots, n\}$. Then there exist a subset $\mathcal{M}_0 \subset \mathcal{N}$, with $\#\mathcal{M}_0 = m$ such that

$$\left| \sum_{k \in \mathcal{M}_0} z_k^\nu \right| \ll_\epsilon m^{1/2+\epsilon}. \quad (\nu = 1, \dots, n^h)$$

Proof. The Lemma is the same as Lemma 9 from [3] except for the fact that $\lfloor \alpha n^2 \rfloor$ is replaced by n^h . The proof is the same, but we need the choice $N > \frac{h}{2\theta\epsilon}$ instead of $N > \frac{1}{\theta\epsilon}$. \square

By the Baker-Harman-Pintz theorem [5] we can choose a prime $n < p$ such that $p - n \asymp p^{0.525}$. By the construction given in Lemma 1, we can choose a p -tuple (z_1, \dots, z_p) of unimodular complex numbers such that

$$\left| \sum_{k=1}^p z_k^\nu \right| \leq (h-1)\sqrt{p}. \quad (\nu = 1, \dots, p^h - 2)$$

Let $m = p - n$. By Lemma 2 with $\theta = 0.525$ and $C = h-1$ we can choose a subset $\mathcal{M}_0 \subset \{1, \dots, p\}$ with $\#\mathcal{M}_0 = m$ such that

$$\left| \sum_{k \in \mathcal{M}_0} z_k^\nu \right| \leq n^{0.2625+\epsilon}. \quad (\nu = 1, \dots, p^h - 2) \quad (\epsilon > 0)$$

Let $\mathcal{N} = \{1, \dots, p\} \setminus \mathcal{M}_0$. It is clear that $\#\mathcal{N} = n$ and by the triangle inequality it follows for $1 \leq \nu \leq n^h \leq p^h - 2$ that

$$\begin{aligned} \left| \sum_{k \in \mathcal{N}} z_k^\nu \right| &= \left| \sum_{k=1}^p z_k^\nu - \sum_{k \in \mathcal{M}_0} z_k^\nu \right|, \\ &= \left| \sum_{k=1}^p z_k^\nu \right| + O\left(\left| \sum_{k \in \mathcal{M}_0} z_k^\nu \right| \right), \\ &\leq (h-1)\sqrt{n + O(n^{0.525})} + O(n^{0.2625+\epsilon}), \\ &\leq (h-1)\sqrt{n} + O(n^{0.2625+\epsilon}). \end{aligned}$$

which finishes the proof of our Theorem. \square

References

- [1] J. Andersson. On some power sum problems of Turán and Erdős. *Acta Math. Hungar.*, 70(4):305–316, 1996.
- [2] J. Andersson. Explicit solutions to certain inf max problems from Turán power sum theory, 2006 [arXiv:math/0607238](#). To Appear in *Indagationes Mathematicae*.
- [3] J. Andersson. Turán’s problem 10 revisited, 2007. [arXiv:math/0609271](#).
- [4] J. Andersson. Lower bounds in some power sum problems, 2007. [arXiv:0704.1879](#).
- [5] R. C. Baker, G. Harman, and J. Pintz. The difference between consecutive primes. II. *Proc. London Math. Soc. (3)*, 83(3):532–562, 2001.
- [6] R. C. Bose. An affine analogue of Singer’s theorem. *J. Indian Math. Soc. (N.S.)*, 6:1–15, 1942.
- [7] R. C. Bose and S. Chowla. Theorems in the additive theory of numbers. *Comment. Math. Helv.*, 37:141–147, 1962/1963.
- [8] F. R. K. Chung. Diameters and eigenvalues *J. Amer. Math. Soc.*, 2:187–196, 1989.
- [9] P. Erdős and A. Rényi. A probabilistic approach to problems of Diophantine approximation. *Illinois J. Math.*, 1:303–315, 1957.
- [10] N. M. Katz. An estimate for character sums. *J. Amer. Math. Soc.*, 2(2):197–200, 1989.
- [11] H. Leenman and R. Tijdeman. Bounds for the maximum modulus of the first k power sums. *Nederl. Akad. Wetensch. Proc. Ser. A* **77**=*Indag. Math.*, 36:387–391, 1974.
- [12] H. L. Montgomery. *Ten lectures on the interface between analytic number theory and harmonic analysis*, volume 84 of *CBMS Regional Conference Series in Mathematics*. Published for the Conference Board of the Mathematical Sciences, Washington, DC, 1994.
- [13] P. Turán. On a certain limitation of eigenvalues of matrices. *Aequationes Math.*, 2:184–189, 1969.

- [14] P. Turán. *On a new method of analysis and its applications*. Pure and Applied Mathematics (New York). John Wiley & Sons Inc., New York, 1984. With the assistance of G. Halász and J. Pintz, With a foreword by Vera T. Sós, A Wiley-Interscience Publication.
- [15] A. Weil. On some exponential sums. *Proc. Nat. Acad. Sci. U.S.A.*, 34:204–207, 1948.